The new police and criminal justice data protection directive

de Hert, Paul; Papakonstantinou, Vagelis

Published in:
New journal of European criminal law

Publication date:
2016

Document Version
Publisher's PDF, also known as Version of record

Mars 12/18

ANALYSIS & OPINION

THE NEW POLICE AND CRIMINAL JUSTICE DATA PROTECTION DIRECTIVE

A First Analysis

PAUL DE HERT and VAGELIS PAPAKONSTANTINOU

1. INTRODUCTION

Allegedly the Police and Criminal Justice Data Protection Directive (henceforth, the "*Directive*") is the little-known, much overlooked part of the EU data protection reform package that stormed into the EU legislative agenda towards the end of 2015. Its counterpart, regulating all other personal data processing activities, the General Data Protection Regulation (henceforth, the "*Regulation*"), is undoubtedly the text that fascinated legislators, legal scholars and even journalists over the four years since their simultaneous release in first draft formats, with its numerous noteworthy novelties: the right to be forgotten, the right to data portability, data protection impact assessments, privacy by design, consistency and one-stop-shop mechanisms among EU Data Protection Authorities etc. Compared to this impressive list the text of the Directive indeed sounds mundane and unimaginative. However, we firmly believe that the repercussions it will have in the EU personal data processing scene surrounding the work of law enforcement authorities, once it comes into effect, will be fundamental and will be equally felt by everybody exactly in the same way that its famous sibling intends to do.

Work on the so-called EU data protection reform package, comprised of the Regulation and the Directive, begun as early as 2009 with the release of a public consultation by the Commission that led to the first Commission position paper being published in 2010 ("*A comprehensive approach on personal data protection in the European Union*", COM(2010) 609 final). Subsequently the Commission released its first drafts on the Regulation and the Directive in early 2012. Over the following years the text was processed by the Council and the Parliament. The Parliament was the first to reach a final position, as early as 2013. The Council, perhaps unburdened by considerations on forthcoming elections, took its time and was able to reach a final position in 2015. The *trilogue* that followed was relatively brief and the final compromise text of the Directive was made known on 15 December 2015, as approved by the Parliament. At the time that this article was drafted the Directive has not yet formally

been adopted and numbered, something that is expected to take place in early summer after the text has also received linguistic processing. Consequently, the wording and the numbering in the analysis that follows may differ slightly from the final text, because the above text improvements are pending. The text used for this report is the final compromise text as released by the Parliament on 15 December 2015.

2. A FEW WORDS ON THE BACKGROUND: THE FRAMEWORK DECISION 977/2008 AND THE CHOICE OF LEGAL INSTRUMENT

The Directive replaces the 2008 Data Protection Framework Decision (henceforth the "*Framework Decision*", see Article 58 of the Directive). This is a replacement that no proponent of data protection will lament. The Framework Decision was a text that was introduced by the Commission with great expectations back in 2008 (namely, in order to constitute for police and criminal justice personal data processing the basic framework, standard-setting text) but was subsequently watered down through long negotiations to the point of near data protection irrelevance; its scope became substantially restricted (only transborder data flows), its principles were worded almost to the point of voluntary application, and its individual rights (information, access and rectification) offered unbalanced priority to the needs of security-related processing. In this way, a text that was released in order to set the data protection standard to the numerous EU personal data protection *ad hoc* instruments released in the aftermath of the first wave of terrorist attacks in EU capitals in practice excused itself from this role (see in particular Article 28).

The new Directive promises to change all of this. After the Treaty of Lisbon came into effect, its Article 16 made an EU data protection overhaul necessary: a new fundamental right, the right to individual data protection, was to be respected and observed at all levels. However, Declaration 21 acknowledges that the specific nature of the security field merits special legislative treatment. The Directive is the response to this new scene in the police and criminal justice context (see also Recitals (1), (8), (10) and (11)); it aims at increasing the level of data protection afforded to individuals and at addressing well-identified shortcomings of the Framework Decision.

The EU law-making policy options and choices are important in their own right. The EU approach, that confirmed the Commission's initial concept, is that processing in the police and criminal justice context needs to be differentiated from all other personal data processing. To this end two instruments, one general and one specifically designed for law enforcement authorities, were introduced instead of one legal instrument encompassing all personal data processing in the EU. In addition, while general personal data processing was considered mature enough to profit from a Regulation, entailing direct effect throughout the EU, police and criminal justice was treated differently: a Directive was the instrument of choice in this case, allowing

Member States a certain level of flexibility while incorporating it into their respective national laws. In this way the EU acknowledged a two-speed process in the effort to harmonise all EU personal data processing.

An important note to be made at this point refers to the special characteristics of police and criminal justice personal data processing. Unlike general personal data processing, processing performed for security-related processing requires a certain level of flexibility. For instance, strict requirements of data quality may not be observed when security data are often based on hearsay, information from undercover sources and rumours. Or, the principle of purpose limitation may not be strictly applied, because information collected on a particular case may find unexpected uses in resolving other cases in the near or not so near future. Or, the right to information and access, if exercised to their fullest extent possible, would practically render any suspect surveillance operation obsolete. This is why special security-related needs have to be accommodated in a relevant data protection text; the task of striking a balance between the data protection purposes and security policy objectives is a sensitive and admittedly difficult one.

Finally, it ought to be made equally clear that the type of personal data processing to be regulated under this Directive is excluded from personal data processing in the context of (criminal) court proceedings. In fact, once a criminal investigation has been opened with the competent authorities, the norm is expected to be (depending of course on the way of implementation into each different Member State national law) that the provisions of this Directive, and the national law implementing it, are automatically disapplied in favour of the applicable Code or Law on Criminal Procedure, according to a relationship of *lex generalis* to *lex specialis* respectively.

3. THE RELATIONSHIP BETWEEN THE DIRECTIVE AND THE REGULATION: SIBLINGS BUT NOT TWINS

Because personal data processing needs and circumstances cannot be foreseen in detail, the relationship between the Directive and the Regulation is important. In particular, there may well be cases where security-related authorities engage in personal data processing that do not fall under the Directive but under the Regulation. The opposite may also be true: agencies that normally undertake general-purpose personal data processing may find themselves involved in processing executed for security purposes. To this end, the Directive clarifies (in Article 7a) that its provisions apply strictly in relation to processing serving its purposes (as expressed in Article 1.1) and also provides some useful guidance (clarifying for instance in Recital (24)) that where data is initially collected by a competent authority for one of the purposes of the Directive, the Regulation should apply to the processing of this data for other purposes), but otherwise leaves the matter to Member States to better define in national law.

Finally, the need for consistency between the texts of the Regulation and the Directive is ever-present in the text of the latter; in fact, every effort has been made for notions, ideas, principles and even structure to be duplicated from the Regulation to the Directive. Attention should be given to the fact that this is a one-way process, meaning from the Regulation towards the Directive, as also depicted in the much more limited attention received by the Directive during its legislative passage (in terms of actual meetings held on it). It is undeniable, as evidenced also in the respective final texts of the two instruments, that references are made in the text of the Directive to the text of the Regulation but not vice versa. This undeclared supremacy of the Regulation, that seems to be perceived as preceding the Directive even by a few hours, may prove important as court challenges on the meaning of the Directive's terms potentially arise in the future. In the same context, Member States are likely to implement the Regulation in a general way, therefore making it the reference text also for law enforcement processing (something ultimately permitted by the Directive, as per its Article 1.1a).

4. THE DIRECTIVE'S SCOPE: ADDRESSING SHORTCOMINGS OF THE PAST, BUT NOT FOR SECRET SERVICES AND EU AGENCIES

The Directive addresses the Framework Decision's gravest shortcoming: its scope is now intended to cover all personal data processing undertaken in the law enforcement (police and criminal justice) context, regardless of whether the processing takes place within or crosses national borders (see Article 2.1 and 1). In this way the Framework Decision's most basic restriction is finally lifted and consequently all security-related authorities within the EU will have to implement the Directive's provisions into their routine personal data processing. Even if that were the Directive's only contribution to the data protection purposes, it would still be cause enough for celebration. The complexity behind this achievement ought not to be overlooked: law enforcement processing practices differ widely among EU Member States, ultimately being connected to issues of history and culture. Differences in technological competences and uses of new technologies in routine police work also widen the EU gap. An effort to harmonise these practices at a level as detailed as that of regulating how they process personal data has never been attempted before. The success in bringing all of the EU Member States' personal data processing for police and criminal justice purposes under a common regulatory framework constitutes one of the Directive's main contributions to the aims of data protection.

On the other hand, as anticipated, the Directive does not apply to the processing of personal data "*in the course of an activity which falls outside the scope of Union law*" (most notably, national security) as well as to processing "*by the Union institutions, bodies, offices and agencies*" (Article 2.3). The latter exemption, expected and justified

on the basis of legal instrument, leaves out of the Directive's scope all of the EU's agencies, bodies and databases entrusted with security-related work (indicatively, Europol, Eurojust, OLAF, the Schengen or Customs Information Systems, etc.) that will apparently continue to apply their, usually *ad hoc*, data protection regimes.

Having noted the above, the Directive's expressed aim for the "*free movement of such data*", as after all included in its title, ought never to escape our attention. The Directive's intention is not to restrict the flow of information among the agencies involved in law enforcement-related personal data processing within the same or even among different Member States. In fact, quite the opposite is true: by introducing a comprehensive data protection legal framework on how to execute such processing and exchange such personal data, the Directive aims at institutionalising and streamlining such data flows. In other words, the aim here is to enable, through regulation, and not to prohibit personal data processing in the police and criminal justice context across the EU.

5. PRINCIPLES AND LAWFULNESS OF THE PROCESSING

As per the basic EU data protection scheme, personal data need to be processed "*lawfully and fairly*". While guidance on the latter term is scarce, what constitutes "*lawful*" processing is explicitly provided for in the relevant legislative texts. In the Regulation altogether six legal bases are set: consent, performance of a contract, compliance with legal obligation, vital interests, public interest, and legitimate interest of the controller (see Article 6). Expectedly however the same legal bases are not included in the text of the Directive (consent, admittedly, would be of little relevance in this case): instead, "*Member States shall provide that the processing of personal data is lawful only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) [the purposes set in the title of the Directive] and is based on Union or Member State law*" (Article 7). In this way in order for the legality of the processing to be established in the case of the Directive only the performance of a task within its scope need occur, as described in the Member State law implementing it.

As described above law enforcement-related personal data processing has special needs and characteristics and the Directive strives to accommodate them as best as possible: while all basic data protection principles are included in its text (for instance, the purpose limitation principle, data quality, data security, etc., see its Article 4) obvious effort has been made to strike a balance between individual data protection and the interests of the police and criminal justice process. For example, with regard to the principle of data quality, "*Member States shall ensure that, as far as possible, personal data based on facts are distinguished from personal data based on personal assessments*" (Article 6). Or, as far as the purpose limitation principle is concerned, "*Member States shall provide that, where applicable and as far as possible, the controller*

makes a clear distinction between personal data of different categories of data subjects" (Article 5). Whether the correct balance has been struck in the exemptions described above is anybody's guess and will very much depend on Member States' implementing legislation and practices; to our mind, however, the Directive's approach is towards the right direction with regard to its aim and purposes.

That being said, there are considerable differences with the basic document on law enforcement processing activities, the 1987 Council of Europe Recommendation 87(15) regulating the use of personal data in the police sector. It would bring us too far but a careful comparison between the new Directive and this older document shows considerable willingness to loosen obligations of law enforcement authorities ensure the normal application of principles. It suffices to see how recital 19 weakens the requirements of Article 4, par. 2 of necessity and proportionality with regard to further use of data. Developments with regard to intelligence-led policing and big data law enforcement have without any doubt contributed to this.

6. RIGHTS OF THE DATA SUBJECT

A basic component of the EU approach to data protection refers to the set of special rights afforded to individuals in order for them to effectively exercise their right to data protection. These are the rights to information, access and rectification. Admittedly, as noted above, if exercised to their fullest extent these rights would undermine much police and criminal justice work. To this end the Directive again attempts to strike a balance between the individual right to data protection and the processing interests and concerns of the police and other law enforcement-related agencies. The rights to information, access and rectification are indeed acknowledged in its text, however in a wording that allows for the level of flexibility required by the type of processing upon which they are to be applied.

The Directive's structure follows that of the Regulation, with the first Article in the respective Chapter (Article 10) laying down the modalities applicable over all of the above individual rights (generally aimed at identifying the data controller as the actor responsible), the analysis of which follows (Articles 11 to 17). As far as the right to information is concerned (Article 10a), the information to be provided to individuals is distinguished into two subsets, of which the second, which is considered more substantial (legal basis of the processing, storage period, recipients), is to be provided only in certain cases and may also be restricted or omitted altogether under certain circumstances (obstructing official or legal inquiries, investigations or procedures, etc.). The right of access (Article 12) is indeed provided to individuals in the known format of obtaining from the data controller information on data kept in its systems, but subject to important limitations (laid down in Article 13, again including the obstruction of official or legal inquiries, investigations or procedures) that could end up easily curtailing its effectiveness for individuals. Finally, the right to "*rectification,*

erasure and restriction of the processing" is acknowledged in Article 16 of the Directive: individuals have the right to request deletion or rectification of their personal data in the event of unlawful processing by the data controller. However, the controller may opt for "*restriction of the processing*" if this seems better suited to its purposes. Here again the ever-present limitation in the event of obstructing official or legal inquiries, investigations or procedures is also included, formulating in essence a basic filter under which all individual rights to information, access and rectification will be exercised. Extensive use therefore of this filter might ultimately render the exercise of all individual rights irrelevant – it will be up to Member States to strike the correct balance within their respective jurisdictions. In the same context, the Directive seems to pay no attention whatsoever to law enforcement systems where only indirect access to information exists.

7. THE ROLE OF DPAS (SUPERVISORY AUTHORITIES) – THE EUROPEAN DATA PROTECTION BOARD

The final pillar of the EU data protection model, together with its basic principles and individual rights as discussed above, refers to the establishment of an independent state authority entrusted with the task of monitoring the application of data protection law within the respective Member State. Data Protection Authorities ("*DPA(s)*") have increased substantially their role and visibility since their introduction through the text of Directive 95/46 so as to become the basic enforcement and monitoring data protection mechanism in the EU today – and an exportable regulatory model to third countries as well (see the analysis that immediately follows). However, in the context of police and criminal justice personal data processing the basic tension between DPAs on the one hand and courts and judicial authorities on the other needs to be settled as an absolute priority: DPAs generally tend to take their monitoring powers seriously, if not expansively, and seek to apply them to all and any personal data processing executed within their respective jurisdictions. Judicial authorities on the other hand rightfully feel that the monitoring by a third party of their personal data processing while executing their duties is unjustified, because they too benefit from institutional independence whilst, after all, upholding the law – including data protection law – is their own mission, if not prerogative. The question therefore in practical terms is whether DPAs may monitor processing done by judicial authorities. If left unaddressed it could undermine the whole Directive, in the sense that Member States may opt to move in one direction or the other depending on their legal systems and preferences, creating a harmonisation nightmare in the process. However, the Directive does provide a clear answer in this regard: the processing of judicial authorities when within their judicial capacity ought not to be affected by its provisions (see, for instance, its Article 17 or Recital 55). However, the authorisation for a higher level of data protection, in its Article 1, is also valid and could ultimately be the cause of problems.

In any event, the Directive formally introduces DPAs, as independent supervisory authorities, in the police and criminal justice personal data processing context. Its Article 39 expressly sets that *"each Member State shall provide that one or more independent public authorities are responsible for monitoring the application of this Directive, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the Union"*. In paragraph 2 it is permitted for this role to be awarded to the same authority established under the Regulation, something that is expected to constitute the norm among Member States. The provisions that follow under the same chapter emphasise its independent status and lay down in detail its tasks and competences.

A significant change brought by the EU data protection reform package into the EU data protection scene refers to the replacement of the Article 29 Data Protection Working Party by the European Data Protection Board. The Party has been a consultative mechanism established under Directive 95/46 that was comprised of representatives of all Member State DPAs and over the past twenty years exercised mostly "*soft*" regulatory power, publishing voluntary opinions and recommendations on all data protection matters of importance within the EU that were however subsequently used as guidance at national level by Member State DPAs, ultimately therefore by its own members. Another important power of the Party was to issue opinions on "adequacy" findings with regard to a third country, in order for personal data to be transmitted to it (see the analysis that immediately follows). The soon-to-be-established Board will replace the Article 29 Working Party but, as far as the Directive is concerned, only in name because essentially it will have the same powers as its predecessor. In other words, while in the Regulation context the Board is expected to hold a central role (essentially, through the consistency mechanism), no such role is provided for under the Directive. This is probably an expected development given the Directive's scope and also the fact that it is a Directive, developing therefore no direct effect at Member State level.

8. TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Under the EU data protection model personal data are not transmitted freely outside its borders. On the contrary, a special filter is introduced for these purposes, that of "adequate" protection: as a general rule, personal information is allowed to be transmitted by an EU Member State to a third country only if the recipient warrants an "adequate" level of protection. What is adequate has been determined over the past twenty years centrally, at Commission level for all Member States: it has been a long and cumbersome process that has led to warranting such status until today only to a handful of countries. Data transmissions to all other countries will have to take place under one of the provided alternatives, namely binding corporate rules or model contracts. This

model however, established under Directive 95/46 is applicable to general purpose personal data processing. Data processing in the police and criminal justice context differs, in that it serves by definition the public interest, it frequently involves urgent requests and, following international crime, it may span several jurisdictions simultaneously. In addition, this being a field left until today outside EU law, practically all Member States have bilateral agreements with third countries permitting the exchange of personal data for law enforcement-related purposes, notwithstanding any "adequacy" finding on the recipients' data protection safeguards. Therefore, here again the Directive had to maintain a careful balance between on the one hand the requirements of police and criminal justice work and existing bilateral agreements and, on the other, the requirement for an increased level of personal data protection.

The Directive's provisions strive to address the above constraints. The basic rule remains that data are transmitted outside the EU even in the police and criminal justice context only after an "adequacy" finding with regard to the recipient (Article 35). However, in order to grant the necessary level of flexibility described above (that is after all present also for general purpose data processing, in the form of binding corporate rules, model contract clauses etc.) special provisions have been introduced on "*transfers by way of appropriate safeguards*" (in Article 37) or "*derogations for specific situations*" (in Article 38). While an analysis of the respective mechanisms lies outside the purposes of this report, here it is enough to be noted that the specific police and criminal justice requirements justify these initiatives. On the other hand, within the same context it should also be noted that the Directive does little to affect bilateral agreements already in place: as per its Article 60, "*international agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to the entry into force of this Directive, and which are in compliance with Union law, applicable prior to the entry into force of this Directive, shall remain in force until amended, replaced or revoked*". Admittedly this wording automatically turns all bilateral agreements into definite term ones, in need of amendment to match the Directive's standards immediately when the first opportunity arises. However, if this prompt to do so is not taken to heart by Member States, who are called upon but not obliged to actively seek to amend bilateral agreements in the foreseeable future, the prolonged existence of those which apply lower standards than the Directive could undermine the whole international data transfers edifice.

9. OTHER NOVELTIES: REGULATING PROFILING AND IMPOSING *PRIVACY BY DESIGN* AND OTHER IDEAS

While the Directive may not have created the sensation that its older sibling caused inside and outside data protection circles over the past few years, this does not mean that its text has been left wanting in terms of data protection novelties and adaptations into the complex contemporary personal data processing environment. Admittedly

such notions as the right to be forgotten or the right to data portability may not be applicable in the police and criminal justice context, however apparently every effort has been undertaken to strengthen the Directive's text against future challenges through incorporation of as many new tools, ideas and best practices as possible.

Profiling holds a prominent place among notions that the Directive took the bold step to address head-on. Profiling is defined as "*any form of automated processing of personal data consisting of using those data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*" (Recital 12a). It is especially problematic in the police and criminal justice context, because if misused it could lead to particularly stressful situations for individuals. It is one thing to create profiles for general purposes personal data processing (to be used, for instance, for marketing or customer management purposes) and another completely to create profiles that are subsequently used for crime prevention and investigation. While the ideal would obviously be for any such processing to be abolished, and to instead judge each individual on its own merits and particularities, law enforcement agencies have long maintained that profiling, if used correctly, is particularly useful while executing their duties. This approach is after all confirmed and validated at EU level, for instance, in the Passenger Name Records Directive that was also recently concluded. In any event, the Directive addresses the issue in a direct way: "*Member States shall provide that a decision based solely on automated processing, including, profiling, which produces an adverse legal effect for the data subject or significantly affects him or her shall be prohibited unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller*" (Article 9). In addition, "*profiling that results in discrimination against individuals on the basis of special categories of personal data referred to in Article 8 shall be prohibited, in accordance with Union law*" (par. 2D). Consequently, profiling is allowed in the police and criminal justice context, even on the basis of sensitive data, subject however to appropriate safeguards for the rights and freedoms of individuals.

Other best practices incorporated in the text of the Directive refer to data breach notifications and the introduction of Data Protection Officers in the police and criminal justice field. With regard to the former, data breach notifications have been known on the data protection scene through their use in the electronic communications field (as first introduced in the ePrivacy Directive) and their contribution to the data protection purposes has been assessed positively. Consequently, their presence in the EU data protection reform package took no-one by surprise. In particular with regard to the police and criminal justice personal data processing data breach notifications are to be served primarily to DPAs (see Article 28 of the Directive) and only "*when the personal data breach is likely to result in a high risk for the rights and freedoms of individuals*" is the controller obliged to notify individuals as well (Article 29). The same

is more or less the case with Data Protection Officers: they have been present in the EU data protection model since Directive 95/46 and their scope has increased in importance in the text of the Regulation. In the police and criminal justice context their introduction remains mainly voluntary, and at any event not applicable for "*courts and other independent judicial authorities when acting in their judicial capacity*" (Article 30).

With regard to novelties, while the list is not as long as in the case of the Regulation, the Directive does try to innovate despite its restrictive subject matter. In this context, data protection measures by design and by default are introduced in Article 19: data protection by design explicitly names pseudonymisation as a possible relevant technical and organisational measure, while data protection by default concerns measures that "*ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of individuals*". Finally, Data Protection Impact Assessments have also been introduced in the text of the Directive as compensating measures for the removal of data controllers' obligation to notify. Instead, the principle of accountability places upon data controllers the burden of implementing on their own initiative appropriate data protection measures in relation to the processing they execute. Data Protection Impact Assessments are listed among such measures: "*where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk for the rights and freedoms of individuals, Member States shall provide that the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data*" (Article 25a). The wording of the Directive is not voluntary: whenever new technologies are used in the police and criminal justice context a Data Protection Impact Assessment needs to be drafted in order to mitigate data protection risks as best as possible (see also paragraph 2 of the same Article).

10. CONCLUSION: FIRST REMARKS ON THE DIRECTIVE

This presentation only aims at highlighting the basic elements of the Directive; detailed analyses of its provisions with particular emphasis both on their effect on police and criminal justice processing routines and on their relationship with other instruments already in effect in the EU Area of Freedom, Security and Justice are evidently necessary in order to properly assess its contribution to the data protection purposes. However, it was the intention of this analysis to showcase the herculean task that was carried out successfully by the EU law-making bodies over the past few years. Quietly and unobserved, away from the public lights that were cast upon the Directive's older sibling, the Regulation, EU law-makers strived under two basic guidelines: first, to bring all police and criminal justice personal data processing executed in the EU under a common data protection legal framework. Second, to strike the correct balance between the conflicting needs of better data protection and better police and

criminal justice work. Both tasks were unprecedented at EU level: efforts until today either only achieved harmonisation on very specific databases or remained high-level and away from day-to-day law enforcement practices at Member State level. We firmly believe that the Directive succeeded in fulfilling both its purposes: the Commission's persistence in introducing a Directive for law enforcement-related processing prevailed, creating hope for a possibly harmonised approach at national level. The basic data protection principles and notions are indeed watered down in the text of the Directive but in a way that was both expected and justified in view of the special processing needs of law enforcement agencies. While one could argue that the actual final provisions of the Directive could have been better in many ways, the fact remains that the EU may now at long last boast of a data protection text that sets the EU (and possibly global in the future) bar for compromise between effective police and criminal justice work and the individual right to data protection.

On the other hand it should be noted that the Directive is friendly, or at least open to, technology-led policing. The fact that prevention is listed among its purposes if combined with the level of flexibility warranted to law enforcement processing, as discussed above, leaves space for data analytics (or, big data) applications in police and law enforcement work. Profiling definitely falls under this category and it is true that the Directive takes bold steps to regulate it. However, profiling is only one of many processing operations based on big data. All other similar operations (data mining, data matching, etc.) simply pass unnoticed by the Directive; its general rules and principles will have to suffice in order to provide an adequate level of data protection. However, we believe that this might not be enough. Technology-led policing is substantially different to general law enforcement personal data processing. It is potentially more harmful to individuals, it usually takes place unnoticed and ultimately involves different technical specifications. All of these points would justify the introduction of special, customised, more effective data protection safeguards. In leaving data analytics out of its focus, the Directive has opened up the possibility for generalised intelligence personal data processing to be undertaken by every law enforcement agency, regardless of whether or not such agencies are specialised or accustomed to such processing, and without any special data protection safeguards. We firmly believe that Member States ought to address this shortcoming while incorporating the Directive into their national law.

BIBLIOGRAPHY

P. De Hert & V. Papakonstantinou, 'The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for', *Computer Law and Security Review*, 2009, Vol. 25, Issue. 5, 403–414

P. De Hert & V. Papakonstantinou, 'The Police and Criminal Justice Data Protection Directive: Comment and Analysis', *Society for Computers & Law. Computers & Law Magazine of the SCL*, 2012, vol. 22, No. 6, 21–25

P. & V. Papakonstantinou, 'The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area', report for the European Parliament, 2014, 40p. via www.europarl.europa.eu/RegData/etudes/STUD/2014/510001/IPOL_STU(2014)510001_EN.pdf. Also published as *Brussels Privacy Hub Working Paper*, 2014, vol. 1, No. 1, 36p. Via www.brusselsprivacyhub.org/Resources/BPH-Working-Paper-VOL1-N1.pdf

P. De Hert, 'The Right to Protection of Personal Data. Incapable of Autonomous Standing in the Basic EU Constituting Documents?' *Utrecht Journal of International and European Law*, 2015, vol. 31 Issue 80, 1–4

P. De Hert & V. Papakonstantinou, 'Repeating the Mistakes of the Past will do Little Good for Air Passengers in the EU: The Comeback of the EU PNR Directive and a Lawyer's Duty to Regulate Profiling', *New Journal of European Criminal Law*, 2015, vol. 6, Issue 2, 160–165

P. Schaar & K. Behn, '*Conflicts between data protection harmonisation and a high level of protection: shortcomings of the European Commission's proposal for a Police and Justice in* H. Aden (ed.), *Police Cooperation in the European Union under the Treaty of Lisbon. Opportunities and Limitations*. Baden Baden: Nomos Verlag. (=Schriftenreihe des Arbeitskreises Europäische Integration e.V. Band 83), 2015, 217–222

E. De Pauw, P. Ponsaers, K van der Vijver, W Bruggeman en P. Deelman, *Technology-led Policing*, Journal of Police Studies, Volume 2011–3 No. 20 (CPS Series), Maklu Publishers

Council of Europe Recommendation 87(15) regulating the use of personal data in the police sector Adopted by the Committee of Ministers on 17 September 1987 via https://wcd.coe.int/

Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, *to be published in the Official Journal* (available via compromise trilogue text, as made available by the LIBE Committee on 15 December 2015)

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, *Official Journal*, 350/60, 30 December 2008

Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *to be published in the Official Journal* available via compromise trilogue text, as made available by the LIBE Committee on 15 December 2015)